# PRIVACY IMPACT ASSESSMENT (PIA)

**PRESCRIBING AUTHORITY**: DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance". Complete this form for Department of Defense (DoD) information systems or electronic collections of information (referred to as an "electronic collection" for the purpose of this form) that collect, maintain, use, and/or disseminate personally identifiable information (PII) about members of the public, Federal employees, contractors, or foreign nationals employed at U.S. military facilities internationally. In the case where no PII is collected, the PIA will serve as a conclusive determination that privacy requirements do not apply to system.

**1. DOD INFORMATION SYSTEM/ELECTRONIC COLLECTION NAME:**

Agile Systems Development Environment (ASDE) IL4

**2. DOD COMPONENT NAME:**

United States Transportation Command

**3. PIA APPROVAL DATE:**

06/03/19

## SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

**a. The PII is:** *(Check one. Note: foreign nationals are included in general public.)*

- [ ] From members of the general public
- [x] From Federal employees and/or Federal contractors
- [ ] From both members of the general public and Federal employees and/or Federal contractors
- [ ] Not Collected *(if checked proceed to Section 4)*

**b. The PII is in a:** *(Check one)*

- [x] New DoD Information System
- [ ] New Electronic Collection
- [ ] Existing DoD Information System
- [ ] Existing Electronic Collection
- [ ] Significantly Modified DoD Information System

**c. Describe the purpose of this DoD information system or electronic collection and describe the types of personal information about individuals collected in the system.**

ASDE is the name of USTRANSCOM's instance in the Amazon Web Services GovCloud. The purpose of our cloud environment is to provide resiliency to the bevy of applications USTC has in several on-premises enclaves. It collects names, work emails, and work phone #s.

**d. Why is the PII collected and/or what is the intended use of the PII?** *(e.g., verification, identification, authentication, data matching, mission-related use, administrative use)*

The PII is collected to create accounts for each individual user. The PII consists of work email, position, and phone number.

**e. Do individuals have the opportunity to object to the collection of their PII?** [ ] Yes [x] No

(1) If "Yes," describe the method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object to the collection of PII.

Work emails are used for account creation.

**f. Do individuals have the opportunity to consent to the specific uses of their PII?** [ ] Yes [x] No

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

There isn't a mechanism for withholding the information and giving them an account.

**g. When an individual is asked to provide PII, a Privacy Act Statement (PAS) and/or a Privacy Advisory must be provided.** *(Check as appropriate and provide the actual wording.)*

- [ ] Privacy Act Statement
- [ ] Privacy Advisory
- [x] Not Applicable

We do not provide a PAS.

**h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component?** *(Check all that apply)*

- [x] Within the DoD Component — Specify. To the ECS Federal support contractor managing accounts

| | | |
|---|---|---|
| ☐ Other DoD Components | Specify. | |
| ☐ Other Federal Agencies | Specify. | |
| ☐ State and Local Agencies | Specify. | |
| ☒ Contractor *(Name of contractor and describe the language in the contract that safeguards PII. Include whether FAR privacy clauses, i.e., 52.224-1, Privacy Act Notification, 52.224-2, Privacy Act, and FAR 39.105 are included in the contract.)* | Specify. | Contractor is ECS Federal.<br>Language:<br>5.2 Cyber Security Compliance: The contractor shall ensure the following cybersecurity policies are in place:<br><br>5.2.1 The Contractor will provide a cloud environment that fully complies or exceeds the security requirements for IL 2, 4, and 5 in the DoD Cloud Computing SRG as appropriate. The Contractor will allow the DoD security team to virtually evaluate the environment prior to the placement of any DoD data in the environment and allow virtual security reviews of the environment during the performance of this contract.<br><br>5.2.2 Controlled Unclassified Information (CUI) contains a number of categories, including, but not limited to the following:<br><br>5.2.2.1 Export Control – Unclassified information concerning certain items, commodities, technology, software or other information whose export could reasonably be expected to adversely affect the United States national security and nonproliferation objectives. This includes dual use items; items identified in export administration regulations, international traffic in arms regulations and the munitions list; license applications; and sensitive nuclear technology information.<br><br>5.2.2.2 Privacy Information – Refers to personal information or, in some cases, personally identifiable information (PII) as defined in Office of Management and Budget (OMB) M-17-12 or "means of identification" as defined in 18 USC §1028(d)(7).<br><br>5.2.2.3 Protected Health Information (PHI) as defined in the Health Insurance Portability and Accountability Act of 1996 (Public Law 104-191), as amended. |
| ☐ Other *(e.g., commercial providers, colleges).* | Specify. | |

**I. Source of the PII collected is**: *(Check all that apply and list all information systems if applicable)*

- ☒ Individuals
- ☐ Databases
- ☐ Existing DoD Information Systems
- ☐ Commercial Systems
- ☐ Other Federal Information Systems

**J. How will the information be collected?** *(Check all that apply and list all Official Form Numbers if applicable)*

- ☒ E-mail
- ☐ Official Form (*Enter Form Number(s) in the box below)*
- ☐ Face-to-Face Contact
- ☐ Paper
- ☐ Fax
- ☐ Telephone Interview
- ☐ Information Sharing - System to System
- ☒ Website/E-Form
- ☐ Other *(If Other, enter the information in the box below)*

The website is on the TRANSCOM Common Development Environment Virtual Desktop Integrator (CDE/VDI). Which is the access point for the cloud. It also has a ticketing system called JIRA which allows users to submit requests for tickets, accounts and other items. The form has several fields:
- Summary: A one or two line summary of the issue
- Select your program: Two drop down menus that allow to pick from preselected choice for organization and program
- Requested User's First Name: The first name of the new user (Not set up by the new user, but by someone with in the program chain)
- Requested User's Middle Initial: Self-explanatory
- Requested User's Last Name: Self-explanatory
- Requested User's Email: Self-explanatory
- Requested User's Phone (optional): Self-explanatory
- Program Manager Name: Name of the Program Manager of the program the new user is on
- Program Manager Email: Self-explanatory
- Program Manager Phone (optional): Self-explanatory
- Requested User's PIV Certificate Principle Name (optional): Name on the PIV cert for the user
- Is Dirty/Ingest Bucket Access Required? with radio Yes/No choice buttons: Determining whether the new user requires that capability
- Requested User's Role/Position: Drop down menu allowing submitter to pick which role the user will perform
- Account Administration Action Type Needed: Drop down menu with a bevy of options to choose from for the account (i.e. create, delete, etc.)
-Description: An open box to describe the nature of the problem the ticket is supposed to correct, or the account that is supposed to be opened

**k. Does this DoD Information system or electronic collection require a Privacy Act System of Records Notice (SORN)?**

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information must be consistent.

[X] Yes [ ] No

If "Yes," enter SORN System Identifier

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or http://dpcld.defense.gov/Privacy/SORNs/

or

If a SORN has not yet been published in the Federal Register, enter date of submission for approval to Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD). Consult the DoD Component Privacy Office for this date

If "No," explain why the SORN is not required in accordance with DoD Regulation 5400.11-R: Department of Defense Privacy Program.

**l. What is the National Archives and Records Administration (NARA) approved, pending or general records schedule (GRS) disposition authority for the system or for the records maintained in the system?**

(1) NARA Job Number or General Records Schedule Authority.

(2) If pending, provide the date the SF-115 was submitted to NARA.

(3) Retention Instructions.

**m. What is the authority to collect information? A Federal law or Executive Order must authorize the collection and maintenance of a system of records. For PII not collected or maintained in a system of records, the collection or maintenance of the PII must be necessary to discharge the requirements of a statue or Executive Order.**

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be similar.
(2) If a SORN does not apply, cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply).

(a) Cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If direct statutory authority or an Executive Order does not exist, indirect statutory authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) If direct or indirect authority does not exist, DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component must be identified.

User completes an online form in order to obtain access to the cloud.

**n. Does this DoD information system or electronic collection have an active and approved Office of Management and Budget (OMB) Control Number?**

Contact the Component Information Management Control Officer or DoD Clearance Officer for this information. This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

☐ Yes ☒ No ☐ Pending

(1) If "Yes," list all applicable OMB Control Numbers, collection titles, and expiration dates.
(2) If "No," explain why OMB approval is not required in accordance with DoD Manual 8910.01, Volume 2, " DoD Information Collections Manual: Procedures for DoD Public Information Collections."
(3) If "Pending," provide the date for the 60 and/or 30 day notice and the Federal Register citation.